

IN THE CLAIMS:

The text of all pending claims, (including withdrawn claims) is set forth below. Cancelled and not entered claims are indicated with claim number and status only. The claims as listed below show added text with underlining and deleted text with ~~strikethrough~~, except where strike-through cannot be easily perceived, in which case the text of any deleted subject matter is shown by being placed within double brackets, as provided in 37 C.F.R. § 1.121(c)(2). The status of each claim is indicated with one of (original), (currently amended), (cancelled), (withdrawn), (new), (previously presented), or (not entered).

1-7. (Cancelled)

8. (currently amended) An encryption device comprising XOR means and nonlinear transform means, said encryption device further comprising:

a random number generator for generating a random number h , where h is an integer between zero and $q-1$;

q sets of fixed mask values $FM_{i,h}$, where q is an integer equal to three or more, wherein equation, $FM_{0,h} = C_h \text{ XOR } L1_0 (FMin_h)$, and $C_h = c_{h,15}c_{h,14} \dots c_{h,0}$, are satisfied, where $FM_{i,h}$ is the i -th fixed value of the h -th set of said q sets of fixed mask values, where $Fmin_h$ ~~$FMin_h$~~ is a selected one of said fixed mask values, and where i is an integer,

q sets of fixed S-box tables, wherein equations, $(c_{0,j} \text{ XOR } c_{1,j}) \vee (c_{1,j} \text{ XOR } c_{2,j}) \vee \dots \vee (c_{q-2,j} \text{ XOR } c_{q-1,j}) = (111 \dots 11)_2$ and $(d_{0,j} \text{ XOR } d_{1,j}) \vee (d_{1,j} \text{ XOR } d_{2,j}) \vee \dots \vee (d_{q-2,j} \text{ XOR } d_{q-1,j}) = (111 \dots 11)_2$ are satisfied, a fixed S-box table before masking is defined as $S[x]$, and i -th masked fixed S-box table is defined as $S_{i,h}[x] = S [x \text{ XOR } c_{h,j}] \text{ XOR } d_{h,j}$ for the j -th fixed value, where j is an integer;

linear transform means $L1_i(x)$ and linear transform means $L2_i(x)$, wherein the linear transform means $L1_i(x)$, the nonlinear transform means with the masked fixed S-box table $S_{i,h}$ and the linear transform means $L2_i(x)$ operate in i -th one of rounds; and

a first selector for selecting one fixed value of the h -th set of said q sets of fixed mask values in response to the random number h ,

said XOR means XORing an input thereto with an XOR of a key with said selected fixed value.

9-34. (Cancelled)

35. (previously presented) The encryption device according to claim 8, characterized

in that the linear transform means $L1_i(x)$ is defined as $L1_i(x) = x$.

36. (previously presented) The encryption device according to claim 8, characterized in that the linear transform means $L2_i(x)$ is defined as $L2_i(x) = \text{MixedColumn}(\text{Shift}(x))$.

37. (previously presented) The encryption device according to claim 8, characterized in that the linear transform means $L2_i(x)$ is defined as $\text{Shift}(x)$.

38. (currently amended) An encryption device comprising XOR means and nonlinear transform means, said encryption device further comprising:

a random number generator for generating a random number h , where h is an integer between zero and $q-1$;

q sets of fixed mask values $FM_{i,h}$, where q is an integer equal to three or more, wherein equations, $FM_{i,h} = C_h \text{ XOR } L1_i(L2_{i-1}(D_h))$ for $i \geq 1$, $C_h = c_{h,15}c_{h,14} \dots c_{h,0}$, and $D_h = d_{h,15}d_{h,14} \dots d_{h,0}$, are satisfied, where i is an integer,

q sets of fixed S-box tables, where equations, $(c_{0,j} \text{ XOR } c_{1,j}) \vee (c_{1,j} \text{ XOR } c_{2,j}) \vee \dots \vee (c_{q-2,j} \text{ XOR } c_{q-1,j}) = (1111 \dots 11)_2$ and $(d_{0,j} \text{ XOR } d_{1,j}) \vee (d_{1,j} \text{ XOR } d_{2,j}) \vee \dots \vee (d_{q-2,j} \text{ XOR } d_{q-1,j}) = (1111 \dots 11)_2$, are satisfied, and a fixed S-box table before masking is defined as $S[x]$ and an i -th masked fixed S-box table is defined as $S_{j,h}[x] = S[x \text{ XOR } c_{h,j}] \text{ XOR } d_{i,j}$ for the j -th fixed value, where j is an integer;

linear transform means $L1_i(x)$ and linear transform means $L2_i(x)$, wherein the linear transform means $L1_i(x)$, the nonlinear transform means with the masked fixed S-box table $S_{j,h}$ and the linear transform means $L2_i(x)$ operate in i -th one of rounds; and

a first selector for selecting one fixed value of the h -th set of said q sets of fixed mask values in response to the random number h ;

said XOR means XORing an input thereto with an XOR of a key with said selected fixed value.

39. (previously presented) The encryption device according to claim 38, characterized in that the linear transform means $L1_i(x)$ is defined as $L1_i(x) = x$.

40. (previously presented) The encryption device according to claim 38, characterized in that the linear transform means $L2_i(x)$ is defined as $L2_i(x) = \text{MixedColumn}(\text{Shift}(x))$.

41. (previously presented) The encryption device according to claim 38,

characterized in that the linear transform means $L2_i(x)$ is defined as $\text{Shift}(x)$.

42-49. (Cancelled)

50. (currently amended) An encryption device comprising XOR means and nonlinear transform means, said encryption device further comprising:

a random number generator for generating a random number h , where h is an integer between zero and $q-1$;

q sets of masked fixed mask values $FM_{i,h}$, where q is an integer equal to three or more, wherein equation, $FM_{0,h} = C_h \text{ XOR } L1_0(FMin_h)$, and $C_h = c_{h,15}c_{h,14} \dots c_{h,0}$, are satisfied, where $FM_{i,h}$ is the i -th fixed value of the h -th set of said q sets of fixed mask values, where $FMin_h$ is a selected one of said fixed mask values, and where i is an integer,

q sets of fixed S-box tables, wherein equations $(c_{0,j} \text{ XOR } c_{1,j}) \vee (c_{1,j} \text{ XOR } c_{2,j}) \vee \dots \vee (c_{q-2,j} \text{ XOR } c_{q-1,j}) = (111 \dots 11)_2$ and $(d_{0,j} \text{ XOR } d_{1,j}) \vee (d_{1,j} \text{ XOR } d_{2,j}) \vee \dots \vee (d_{q-2,j} \text{ XOR } d_{q-1,j}) = (111 \dots 11)_2$ are satisfied, a fixed S-box table before masking is defined as $S[x]$, and i -th masked fixed S-box table is defined as $S_{j,h}[x] = \{S[x \text{ XOR } c_{h,j}] \text{ XOR } d_{j,h}\}$ for the j -th fixed value, where j is an integer;

a selector for selecting one of said q sets of fixed S-box tables in response to the random number h ,

said nonlinear transform means nonlinearly transforming an input thereto in accordance with said selected set of fixed S-box tables; and

a plurality of encrypting rounds, wherein i -th one of said plurality of encrypting rounds comprises the XOR means, the fixed S-box tables, the selector, linear transform means $L1_i(x)$ and linear transform means $L2_i(x)$, for that round, and wherein the fixed S-box tables for said plurality of respective encrypting rounds are identical, and wherein the linear transform means $L1_i(x)$, the nonlinear transform means with the masked fixed S-box table $S_{j,h}$ and the linear transform means $L2_i(x)$ operate in that round.

51. (previously presented) The encryption device according to claim 50, characterized in that the linear transform means $L1_i(x)$ is defined as $L1_i(x) = x$.

52. (previously presented) The encryption device according to claim 50, characterized in that the linear transform means $L2_i(x)$ is defined as $L2_i(x) = \text{MixedColumn}(\text{Shift}(x))$.

53. (previously presented) The encryption device according to claim 50, characterized in that the linear transform means $L2_i(x)$ is defined as $\text{Shift}(x)$.

54. (currently amended) An encryption device comprising XOR means and nonlinear transform means, said encryption device further comprising:

a random number generator for generating a random number h , where h is an integer between zero and $q-1$;

q sets of masked fixed mask values $FM_{i,h}$, where q is an integer equal to three or more, wherein equations, $FM_{i,h} = C_h \text{ XOR } L_{-1,j}(L_{-2,j}(\dots(L_{-i,j}(D_h)))$ for $i \geq 1$, $C_h = c_{h,15}c_{h,14}\dots c_{h,0}$, and $D_h = d_{h,15}d_{h,14}\dots d_{h,0}$, are satisfied, where $FM_{i,h}$ is the i -th fixed value of the h -th set of said q sets of fixed mask values, where i is an integer,

q sets of fixed S-box tables, wherein equations, $(c_{0,j} \text{ XOR } c_{1,j}) \vee (c_{1,j} \text{ XOR } c_{2,j}) \vee \dots \vee (c_{q-2,j} \text{ XOR } c_{q-1,j}) = (111\dots 11)_2$ and $(d_{0,j} \text{ XOR } d_{1,j}) \vee (d_{1,j} \text{ XOR } d_{2,j}) \vee \dots \vee (d_{q-2,j} \text{ XOR } d_{q-1,j}) = (111\dots 11)_2$ are satisfied, a fixed S-box table before masking is defined as $S[x]$, and i -th masked fixed S-box table is defined as $S_{i,h}[x] = \{S[x \text{ XOR } c_{h,j}] \text{ XOR } d_{h,j}\}$ for the j -th fixed value, where j is an integer;

a selector for selecting one of said q sets of fixed S-box tables in response to the random number h ,

said nonlinear transform means nonlinearly transforming an input thereto in accordance with said selected set of fixed S-box tables; and

a plurality of encrypting rounds, wherein i -th one of said plurality of encrypting rounds comprises the XOR means, the fixed S-box tables, the selector, linear transform means $L1_i(x)$ and linear transform means $L2_i(x)$, for that round, and wherein the fixed S-box tables for said plurality of respective encrypting rounds are identical, and wherein the linear transform means $L1_i(x)$, the nonlinear transform means with the masked fixed S-box table $S_{i,h}$ and the linear transform means $L2_i(x)$ operate in that round.

55. (previously presented) The encryption device according to claim 54, characterized in that the linear transform means $L1_i(x)$ is defined as $L1_i(x) = x$.

56. (previously presented) The encryption device according to claim 54, characterized in that the linear transform means $L2_i(x)$ is defined as $L2_i(x) = \text{MixedColumn}(\text{Shift}(x))$.

57. (previously presented) The encryption device according to claim 54, characterized in that the linear transform means $L2_i(x)$ is defined as $\text{Shift}(x)$.

58-63. (Cancelled)

64. (currently amended) An encryption device comprising a random number generator for generating a random number h , where h is an integer between zero and $q-1$, and a first plurality of encrypting rounds, wherein

i -th one of said plurality of encrypting rounds comprises nonlinear transform means for nonlinearly transforming an input thereto, and XOR means for XORing a first input thereto with a second input thereto for that round, where i is an integer;

the second input to said XOR means is coupled to an output of said nonlinear transform means; and

said nonlinear transform means comprises:

q sets of fixed mask values $FM_{i,h}$, where q is an integer equal to three or more, wherein equations, $FM_{0,h} = C_h \text{ XOR } L1_0(FMin_h)$, and $C_h = c_{h,15}c_{h,14} \dots c_{h,0}$, are satisfied, where $FM_{i,h}$ is the i -th fixed value of the h -th set of said q sets of fixed mask values, where $FMin_h$ is a selected one of said fixed mask values, and,

q sets of fixed S-box tables, wherein equations, $(c_{0,j} \text{ XOR } c_{1,j}) \vee (c_{1,j} \text{ XOR } c_{2,j}) \vee \dots \vee (c_{q-2,j} \text{ XOR } c_{q-1,j}) = (111 \dots 11)_2$ and $(d_{0,j} \text{ XOR } d_{1,j}) \vee (d_{1,j} \text{ XOR } d_{2,j}) \vee \dots \vee (d_{q-2,j} \text{ XOR } d_{q-1,j}) = (111 \dots 11)_2$ are satisfied, a fixed S-box table before masking is defined as $S[x]$, and i -th masked fixed S-box table is defined as $S_{j,h}[x] = \{S[x \text{ XOR } c_{h,j}] \text{ XOR } d_{j,h}\}$ for the j -th fixed value, where j is an integer;

a selector for selecting one of said q sets of fixed mask values in response to the random number h ;

further XOR means for XORing an input thereto with an XOR of a key with said selected fixed value;

linear transform means $L1_i(x)$;

a plurality of nonlinear transform means for nonlinearly transforming an input in accordance with a fixed S-box table;

linear transform means $L2_i(x)$, wherein the linear transform means $L1_i(x)$, the nonlinear transform means with the masked fixed S-box table $S_{j,h}$ and the linear transform means $L2_i(x)$ operate in that round; and

a selector for selecting one of said plurality of nonlinear transform means.

65. (previously presented) The encryption device according to claim 64, characterized in that the linear transform means $L1_i(x)$ is defined as $L1_i(x) = x$.

66. (previously presented) The encryption device according to claim 64, characterized in that the linear transform means $L2_i(x)$ is defined as $L2_i(x) = \text{MixedColumn}(\text{Shift}(x))$.

67. (previously presented) The encryption device according to claim 64, characterized in that the linear transform means $L2_i(x)$ is defined as $\text{Shift}(x)$.

68. (currently amended) An encryption device comprising a random number generator for generating a random number h , where h is an integer between zero and $q-1$, and a first plurality of encrypting rounds, wherein

i -th one of said plurality of encrypting rounds comprises nonlinear transform means for nonlinearly transforming an input thereto, and XOR means for XORing a first input thereto with a second input thereto for that round, where i is an integer;

the second input to said XOR means is coupled to an output of said nonlinear transform means; and

said nonlinear transform means comprises:

q sets of fixed mask values $FM_{i,h}$, where q is an integer equal to three or more, wherein equations $\{ FM_{i,h} = C_h \text{ XOR } L1_i(L2_{i-1}(D_h)) \text{ for } i \geq 1, C_h = c_{h,15}c_{h,14} \dots c_{h,0}, \text{ and } D_h = d_{h,15}d_{h,14} \dots d_{h,0}, \text{ are satisfied, where } FM_{i,h} \text{ is the } i\text{-th fixed value of the } h\text{-th set of said } q \text{ sets of fixed mask values,}$

q sets of fixed S-box tables, wherein equations $\{ (c_{0,j} \text{ XOR } c_{1,j}) \vee (c_{1,j} \text{ XOR } c_{2,j}) \vee \dots \vee (c_{q-2,j} \text{ XOR } c_{q-1,j}) = (111 \dots 11)_2 \text{ and } (d_{0,j} \text{ XOR } d_{1,j}) \vee (d_{1,j} \text{ XOR } d_{2,j}) \vee \dots \vee (d_{q-2,j} \text{ XOR } d_{q-1,j}) = (111 \dots 11)_2 \text{ are satisfied, a fixed S-box table before masking is defined as } S[x], \text{ and } i\text{-th masked fixed S-box table is defined as } S_{i,h}[x] = \{ S[x \text{ XOR } c_{h,j}] \text{ XOR } d_{h,j} \text{ for the } j\text{-th fixed value, where } j \text{ is an integer;}$

a selector for selecting one of said q sets of fixed mask values in response to the random number h ;

further XOR means for XORing an input thereto with an XOR of a key with said selected fixed value;

linear transform means $L1_i(x)$;

a plurality of nonlinear transform means for nonlinearly transforming an input in accordance with a fixed S-box table;

linear transform means $L2_i(x)$, wherein the linear transform means $L1_i(x)$, the nonlinear transform means with the masked fixed S-box table $S_{i,h}$ and the linear transform means $L2_i(x)$ operate in that round; and

a selector for selecting one of said plurality of nonlinear transform means.

69. (previously presented) The encryption device according to claim 68, characterized in that the linear transform means $L1_i(x)$ is defined as $L1_i(x) = x$.

70. (previously presented) The encryption device according to claim 68, characterized in that the linear transform means $L2_i(x)$ is defined as $L2_i(x) =$

MixedColumn(Shift(x)).

71. (previously presented) The encryption device according to claim 68, characterized in that the linear transform means $L2_i(x)$ is defined as Shift(x).

72. (currently amended) A program stored on a computer or machine-readable storage medium for use in an encryption device, said program operable to effect the steps of:

selecting one set of q sets of fixed mask values $FM_{i,h}$, where q is an integer equal to three or more, in response to a random number h , where h is an integer between zero and $q-1$;

XORing an input value with an XOR of a key with said selected fixed value in i -th one of rounds, wherein equations, $FM_{0,h} = C_h \text{ XOR } L1_0(FMin_h)$ and $C_h = c_{h,15}c_{h,14} \dots c_{h,0}$, are satisfied, where $FM_{i,h}$ is the i -th fixed value of the h -th set of said q sets of fixed mask values, where $FMin_h$ is a selected one of said fixed mask values and where i is an integer;

selecting one set $S_{j,h}$ of q sets of masked fixed S-box tables in response to the random number h in that round, wherein equations, $(c_{0,j} \text{ XOR } c_{1,j}) \vee (c_{1,j} \text{ XOR } c_{2,j}) \vee \dots \vee (c_{q-2,j} \text{ XOR } c_{q-1,j}) = (111 \dots 11)_2$ and $(d_{0,j} \text{ XOR } d_{1,j}) \vee (d_{1,j} \text{ XOR } d_{2,j}) \vee \dots \vee (d_{q-2,j} \text{ XOR } d_{q-1,j}) = (111 \dots 11)_2$ are satisfied, a fixed S-box table before masking is defined as $S[x]$, and i -th masked fixed S-box table is defined as $S_{j,h}[x] = \{S[x \text{ XOR } c_{h,j}] \text{ XOR } d_{j,h}\}$ for the j -th fixed value, where j is an integer;

nonlinearly transforming an input value in accordance with said selected set $S_{j,h}$ of fixed S-box tables in that round; and

linearly transforming an input value and the nonlinearly transformed value in that round.